EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

Overview

Plaintiff accuses Defendant of infringement through making, using, selling, offering for sale, and importation of Zoho's ("Defendant" or "Zoho") ManageEngine, including Endpoint Central and Vulnerability Manager Plus (the "Accused System and Method"), and all substantially similar products. The term "Accused System and Method" includes the associated computer hardware, interfaces, software, and data, and the processes and methods related thereto.

The Accused System and Method is accused of directly infringing U.S. Patent No. 10,893,066 (the"'066 Patent"). Plaintiff further accuses Defendant of indirectly infringing the '066 Patent by providing its customers and others the Accused System and Method to utilize in an infringing manner. Defendant intends to cause infringement by its customers and users as Defendant instructs users to use the Accused System and Method in an infringing manner. Defendant deploys client software to implement the Accused System and Method. Defendant also provides support and implementation services for the Accused System and Method, including providing instructions, guides, online materials, and technical support.

The asserted claims include elements that are implemented, at least in part, by proprietary electronics and software in the Accused System and Method. The precise designs, processes, and algorithms used in them are held secret, at least in part, and are not publicly available in their entirety. An analysis of Defendant's documentation and/or source code may be necessary to fully and accurately describe all infringing features and functionality of the Accused System and, accordingly, Plaintiff reserves the right to supplement these contentions once such information is made available to Plaintiff. Furthermore, Plaintiff reserves the right to revise these contentions, including as discovery in the case progresses, in view of the Court's final claim construction in this action and in connection with the provision of its expert reports.

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

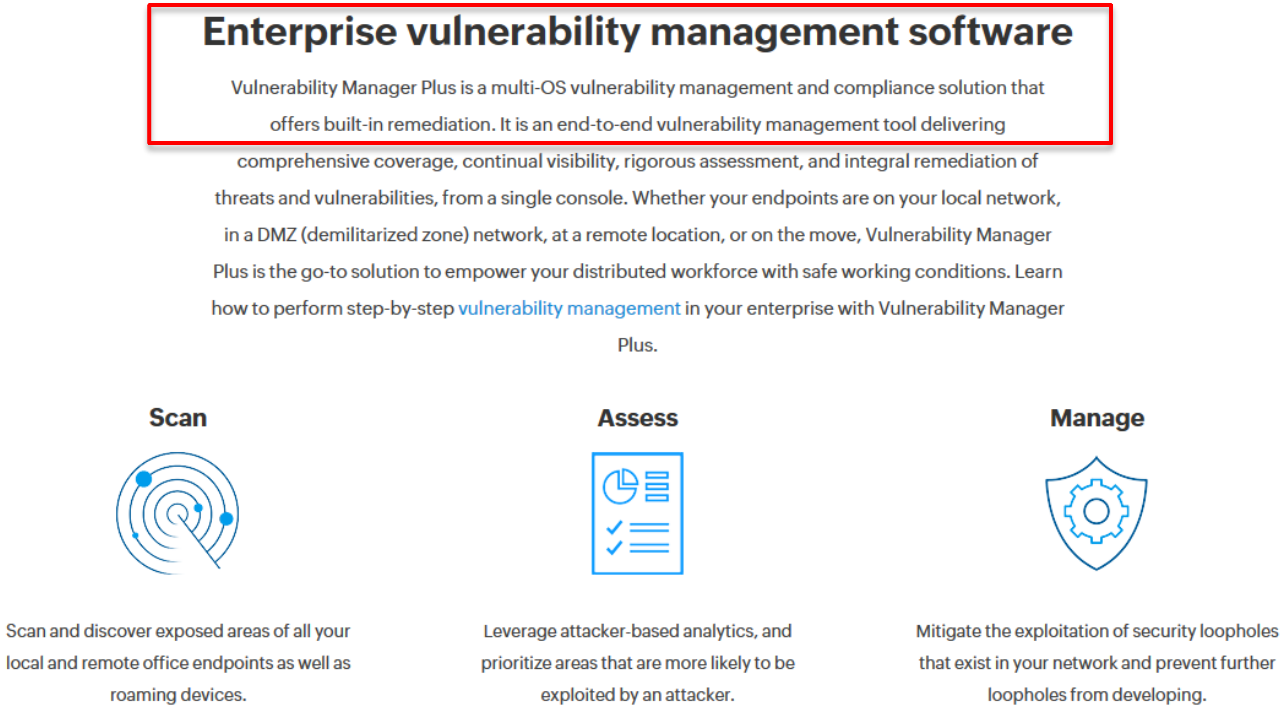
10,893,066 Claim 1	**Evidence**
A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:	ManageEngine includes *a non-transitory computer-readable media storing instructions that, when executed by one or more processors* (e.g., the system on which the management software is operated) **Note:** See, for example, the evidence below (emphasis added, if any):  Enterprise vulnerability management software Vulnerability Manager Plus is a multi-OS vulnerability management and compliance solution that offers built-in remediation. It is an end-to-end vulnerability management tool delivering comprehensive coverage, continual visibility, rigorous assessment, and integral remediation of threats and vulnerabilities, from a single console. Whether your endpoints are on your local network, in a DMZ (demilitarized zone) network, at a remote location, or on the move, Vulnerability Manager Plus is the go-to solution to empower your distributed workforce with safe working conditions. Learn how to perform step-by-step vulnerability management in your enterprise with Vulnerability Manager Plus. Scan Scan and discover exposed areas of all your local and remote office endpoints as well as roaming devices. Assess Leverage attacker-based analytics, and prioritize areas that are more likely to be exploited by an attacker. Manage Mitigate the exploitation of security loopholes that exist in your network and prevent further loopholes from developing. https://www.manageengine.com/vulnerability-management/?pos=EndpointCentral&loc=ProdMenu&cat=UEMS

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

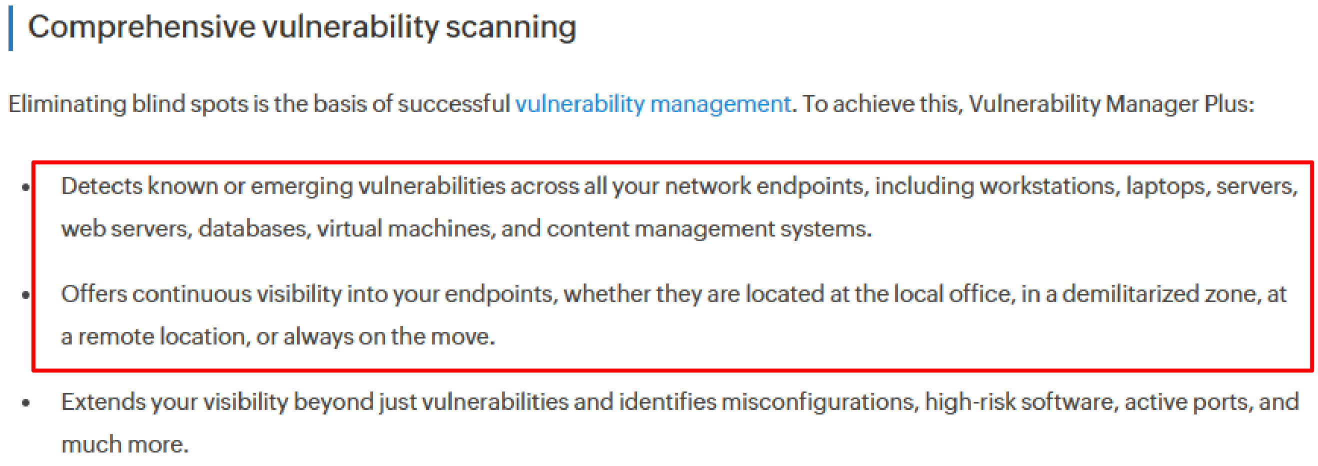
	 Comprehensive vulnerability scanning Eliminating blind spots is the basis of successful vulnerability management. To achieve this, Vulnerability Manager Plus: • Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems. • Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move. • Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more. https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

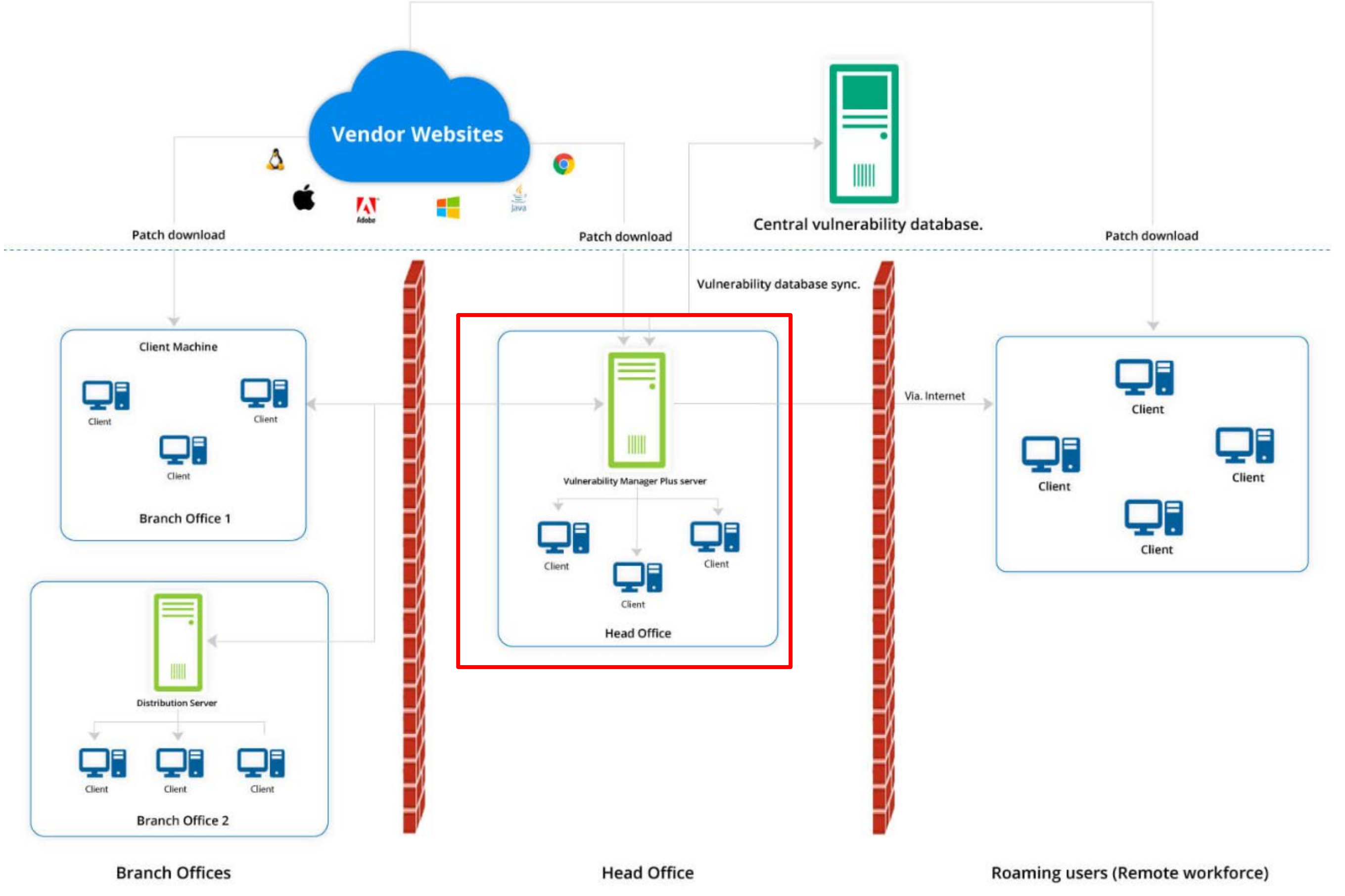
	 Vendor Websites Adobe Java Patch download Patch download Central vulnerability database. Patch download Vulnerability database sync. Client Machine Client Client Client Branch Office 1 Vulnerability Manager Plus server Client Client Client Head Office Via. Internet Client Client Client Client Distribution Server Client Client Client Branch Office 2 Branch Offices Head Office Roaming users (Remote workforce) https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg
receive first vulnerability information from at least one first data storage that is	ManageEngine includes instructions to *receive first vulnerability information from at least one first data storage* (e.g., The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management) *that is generated utilizing second vulnerability information from at*

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

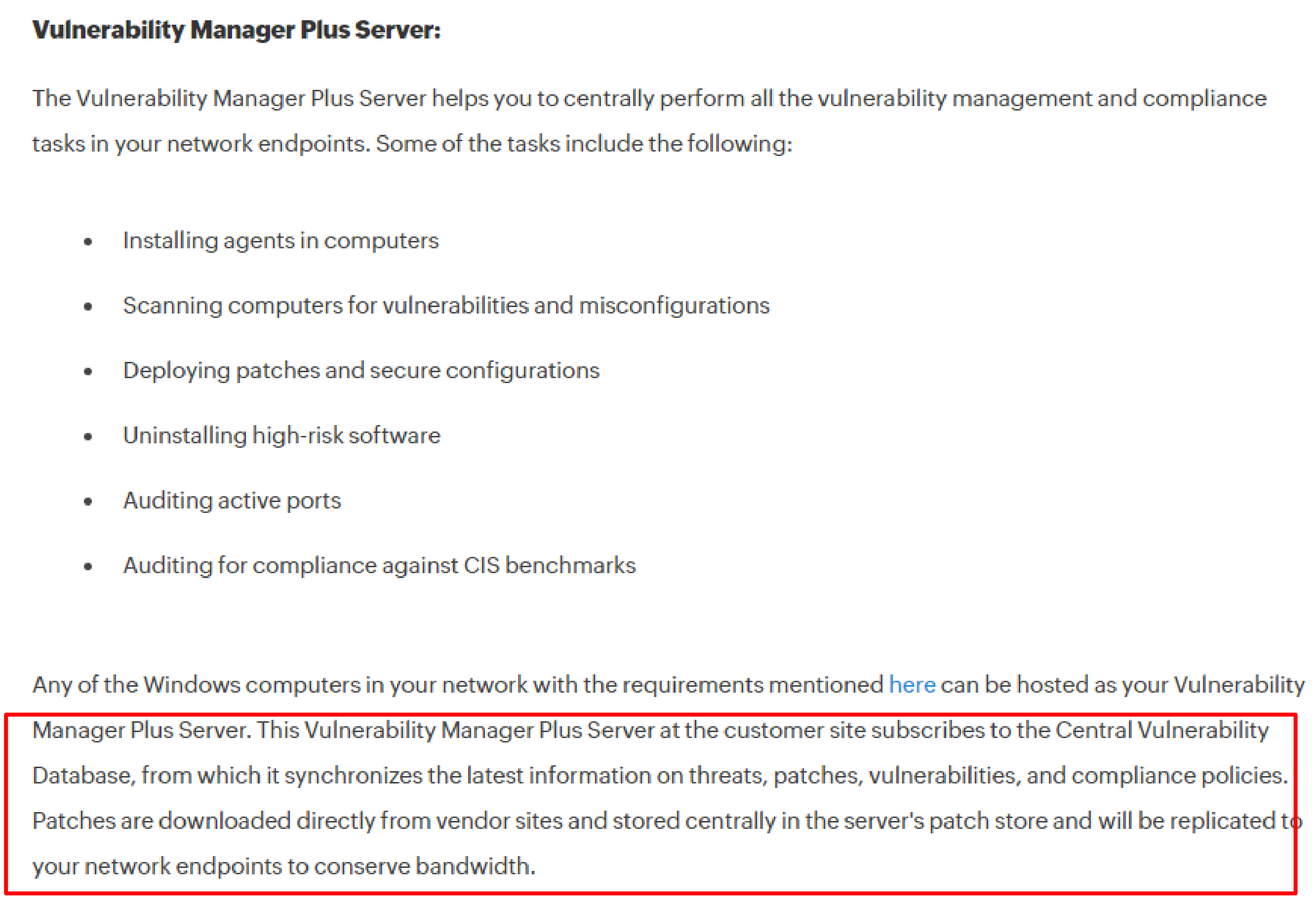
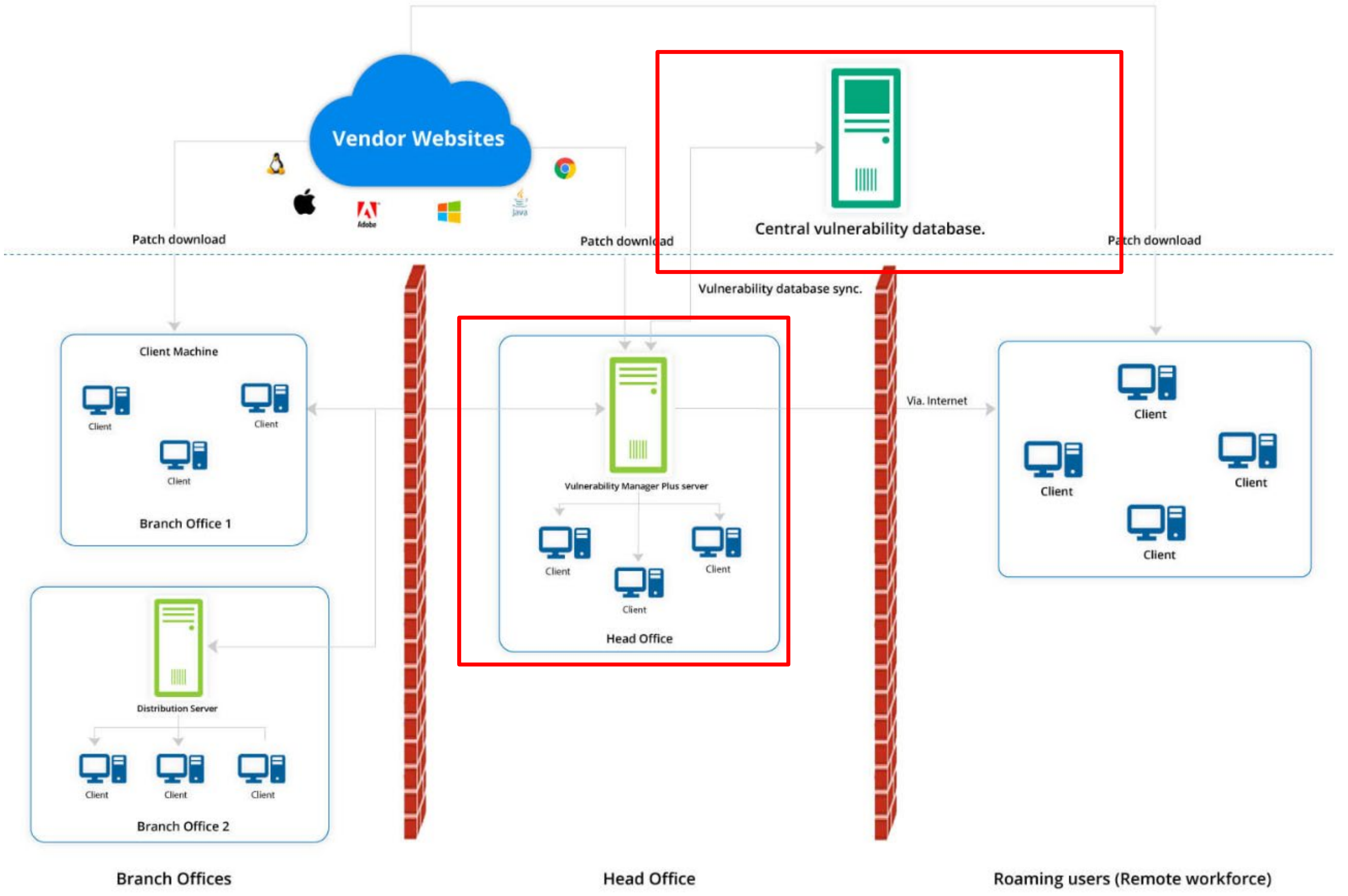
generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;	*least one second data storage* (e.g., a Central Vulnerability Database) *that is used to identify a plurality of potential vulnerabilities* (e.g., a Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console). Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):  **Vulnerability Manager Plus Server:** The Vulnerability Manager Plus Server helps you to centrally perform all the vulnerability management and compliance tasks in your network endpoints. Some of the tasks include the following: • Installing agents in computers • Scanning computers for vulnerabilities and misconfigurations • Deploying patches and secure configurations • Uninstalling high-risk software • Auditing active ports • Auditing for compliance against CIS benchmarks Any of the Windows computers in your network with the requirements mentioned here can be hosted as your Vulnerability Manager Plus Server. This Vulnerability Manager Plus Server at the customer site subscribes to the Central Vulnerability Database, from which it synchronizes the latest information on threats, patches, vulnerabilities, and compliance policies. Patches are downloaded directly from vendor sites and stored centrally in the server's patch store and will be replicated to your network endpoints to conserve bandwidth.

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

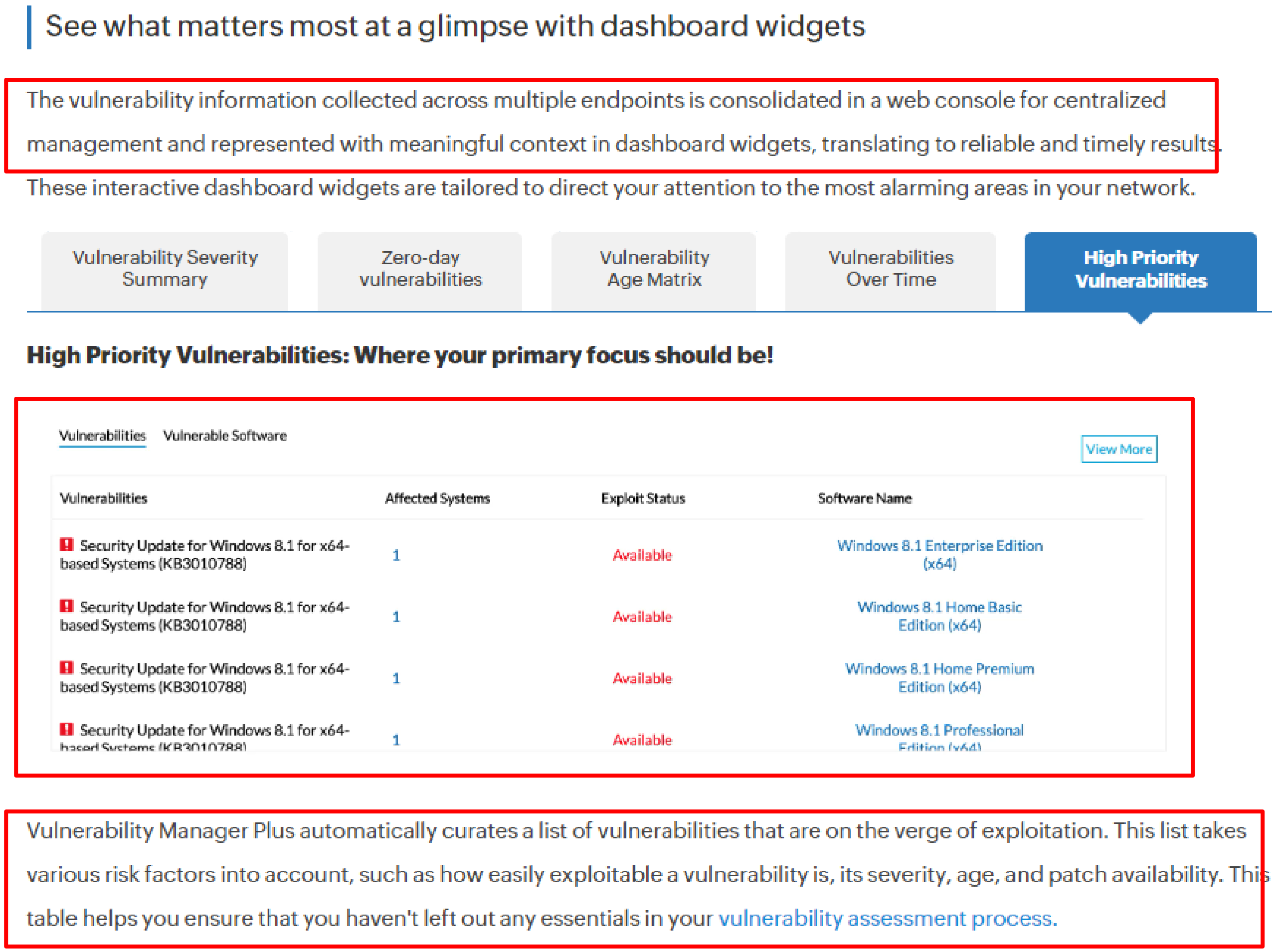
https://www.manageengine.com/vulnerability-management/help/vulnerability-management-architecture.html#v1



https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho



See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results. These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity Summary
Zero-day vulnerabilities
Vulnerability Age Matrix
Vulnerabilities Over Time
High Priority Vulnerabilities

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities	Affected Systems	Exploit Status	Software Name
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your vulnerability assessment process.

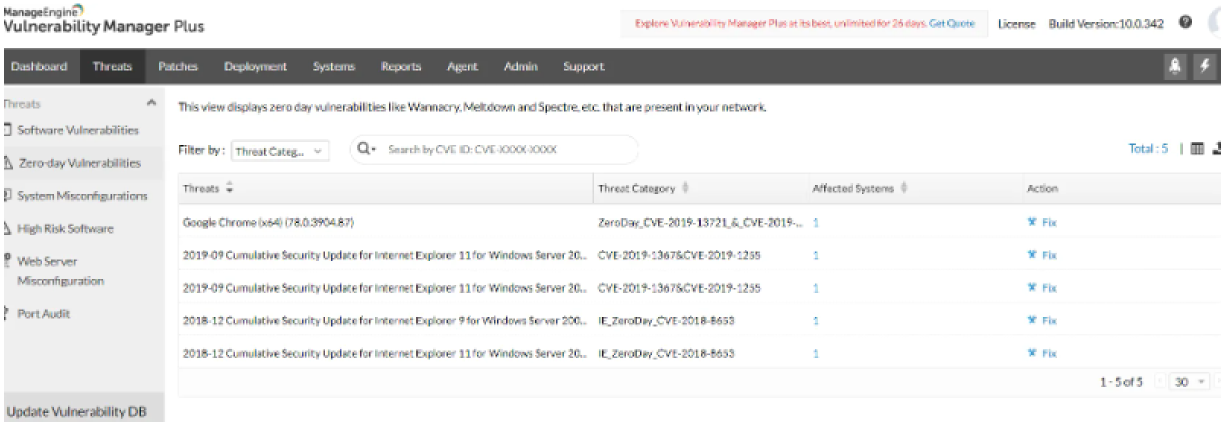
https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

Leverage a dedicated view for zero-days

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.



This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_&_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-1367&CVE-2019-1255	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-1367&CVE-2019-1255	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network. Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. *Subscribe to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news*

https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

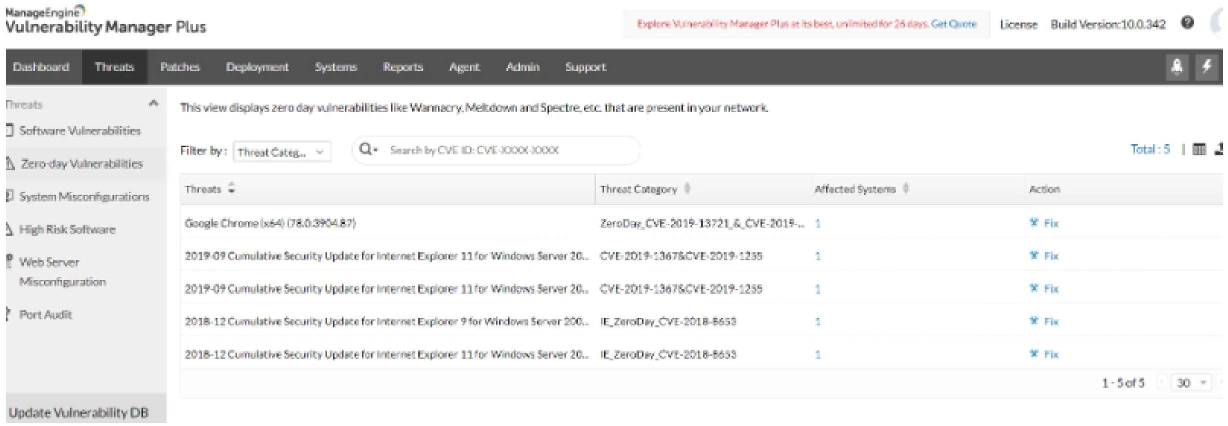
said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;	ManageEngine includes instructions to receive *first vulnerability information generated utilizing the second vulnerability information* (e.g., The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and is generated using information available on a Central Vulnerability Database) *identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device* (e.g., The vulnerability information collected across multiple endpoints). *determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;*(e.g., scan the system on the basis of the vulnerability definition stored on Central Vulnerability Database) Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

Leverage a dedicated view for zero-days

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.



This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_&_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-1367&CVE-2019-1255	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-1367&CVE-2019-1255	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network. Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. *Subscribe to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news*

https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

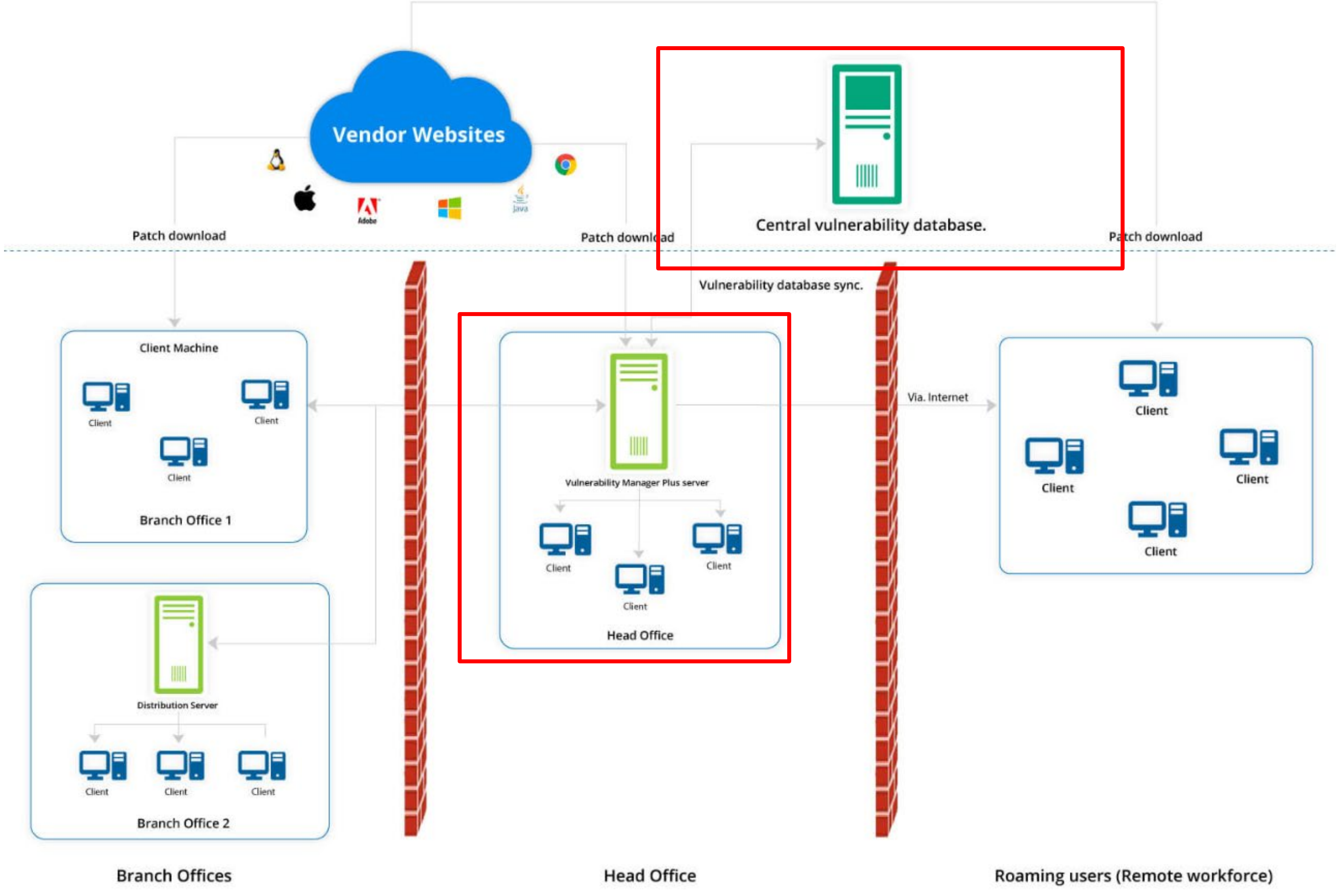
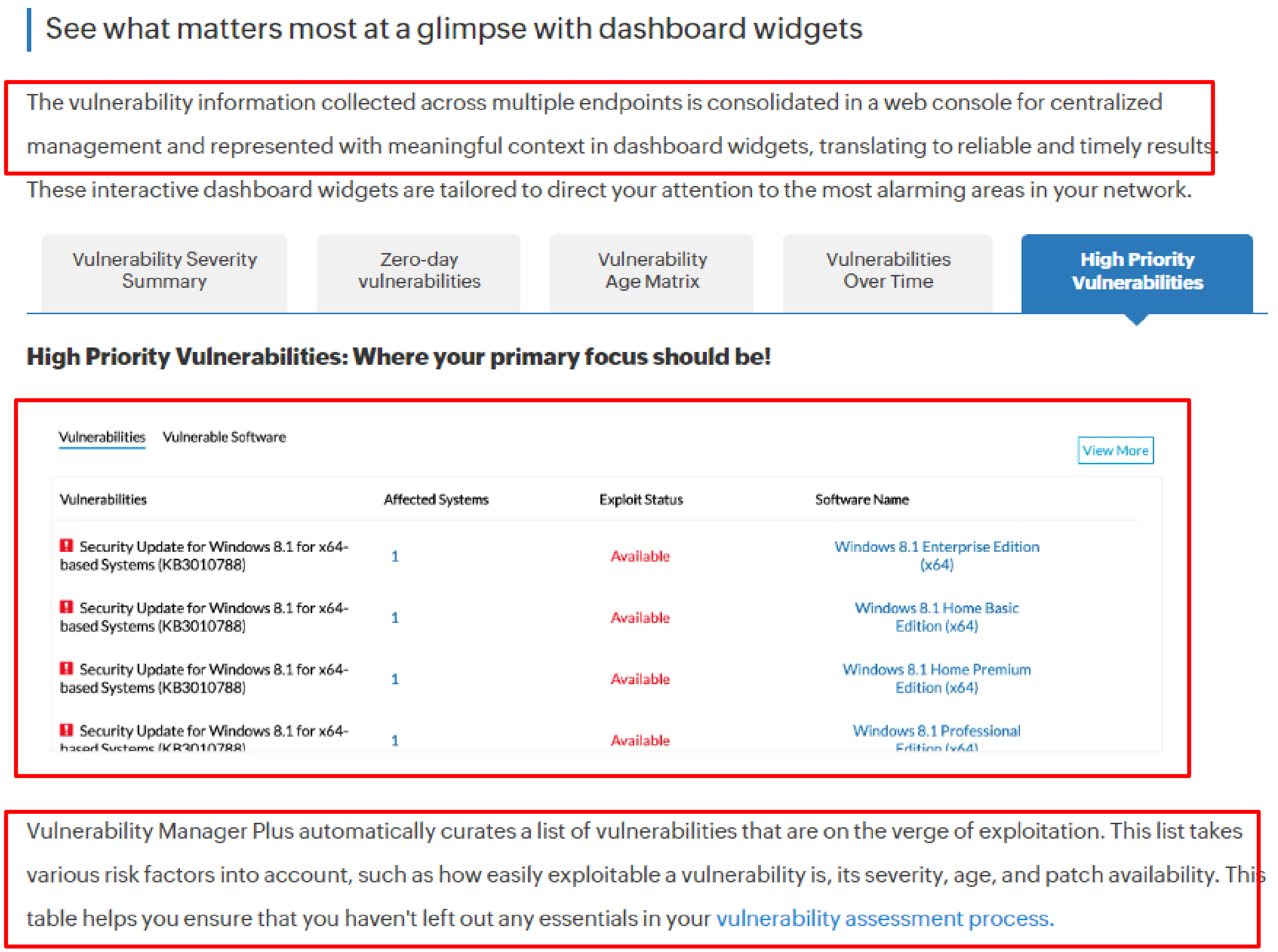
	 Vendor Websites Adobe Java Patch download Patch download Patch download Central vulnerability database. Vulnerability database sync. Client Machine Client Client Client Branch Office 1 Vulnerability Manager Plus server Client Client Client Head Office Via. Internet Client Client Client Client Distribution Server Client Client Client Branch Office 2 Branch Offices Head Office Roaming users (Remote workforce) https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho



See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results. These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity Summary
Zero-day vulnerabilities
Vulnerability Age Matrix
Vulnerabilities Over Time
High Priority Vulnerabilities

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities	Affected Systems	Exploit Status	Software Name
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your vulnerability assessment process.

https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html

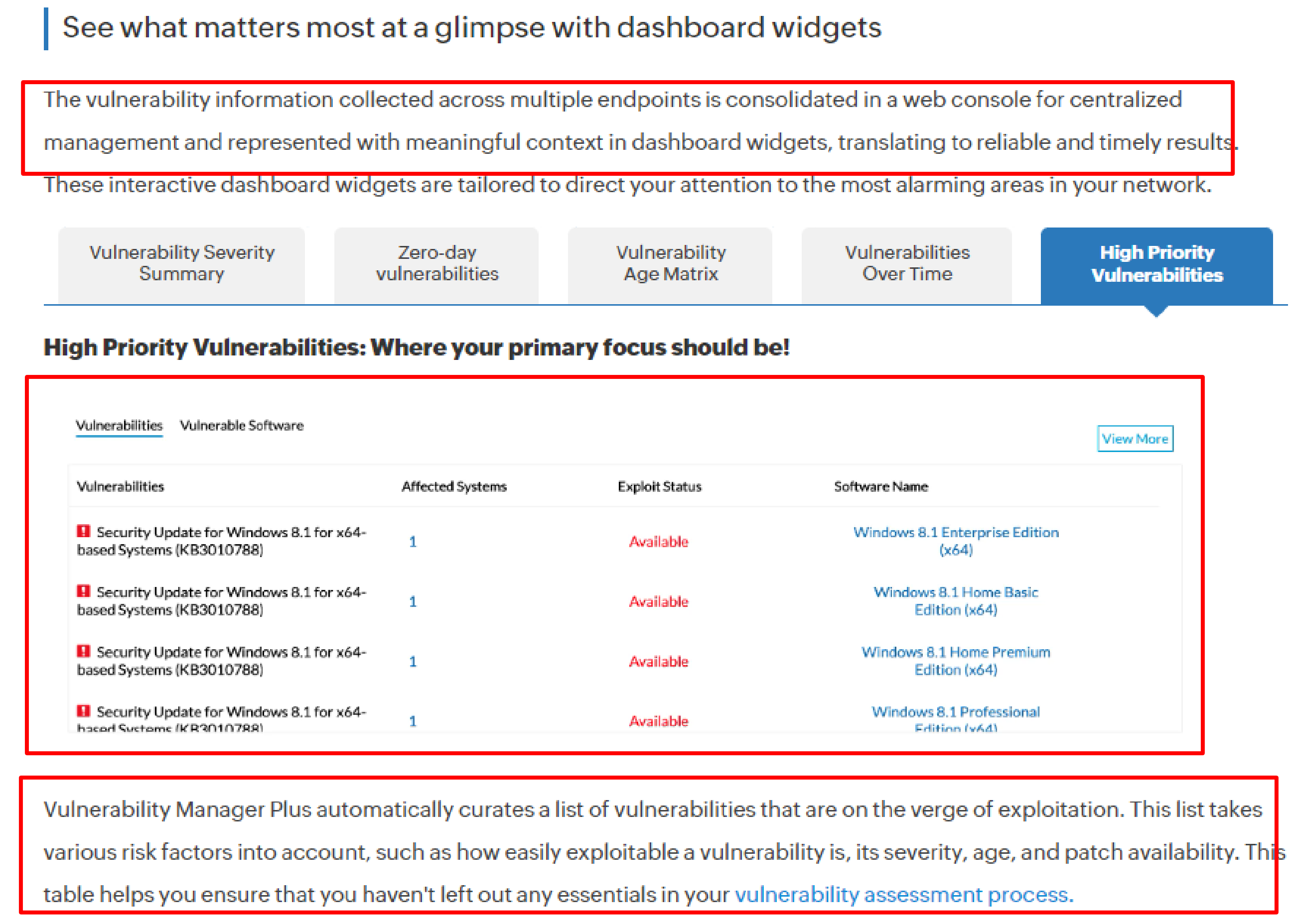
EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

identify an occurrence in connection with at least one of the plurality of devices;	ManageEngine includes instructions to *identify an occurrence in connection with at least one of the plurality of devices* (e.g., The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management) Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho



See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results. These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity Summary
Zero-day vulnerabilities
Vulnerability Age Matrix
Vulnerabilities Over Time
High Priority Vulnerabilities

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities	Affected Systems	Exploit Status	Software Name
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your vulnerability assessment process.

https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html

determine that the at least one actual vulnerability of the at least one of the plurality of	ManageEngine *determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information* (e.g., The vulnerability

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

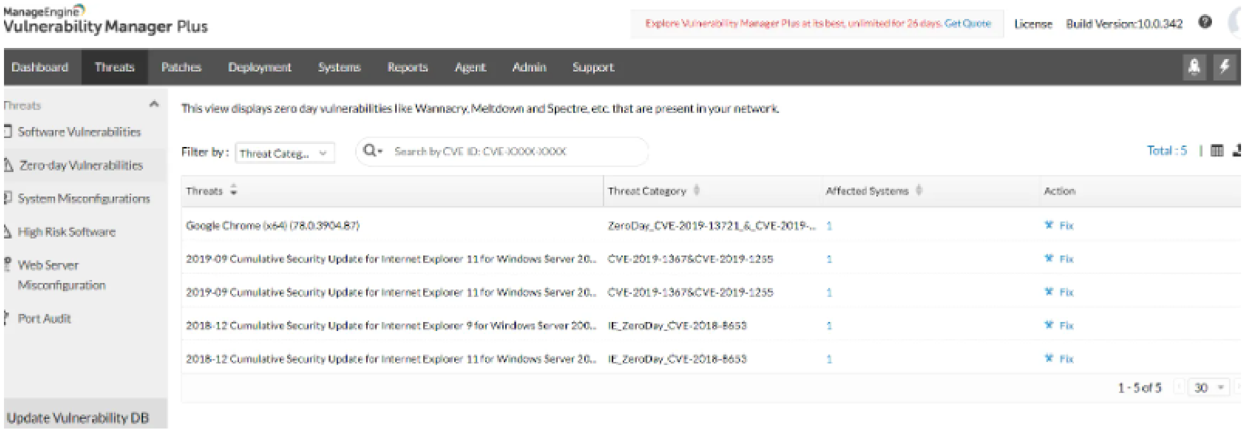
devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and	information collected across multiple endpoints is consolidated in a web console for centralized management) Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

Leverage a dedicated view for zero-days

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.



This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_&_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-1367&CVE-2019-1255	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-1367&CVE-2019-1255	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. *Subscribe to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news*

https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html

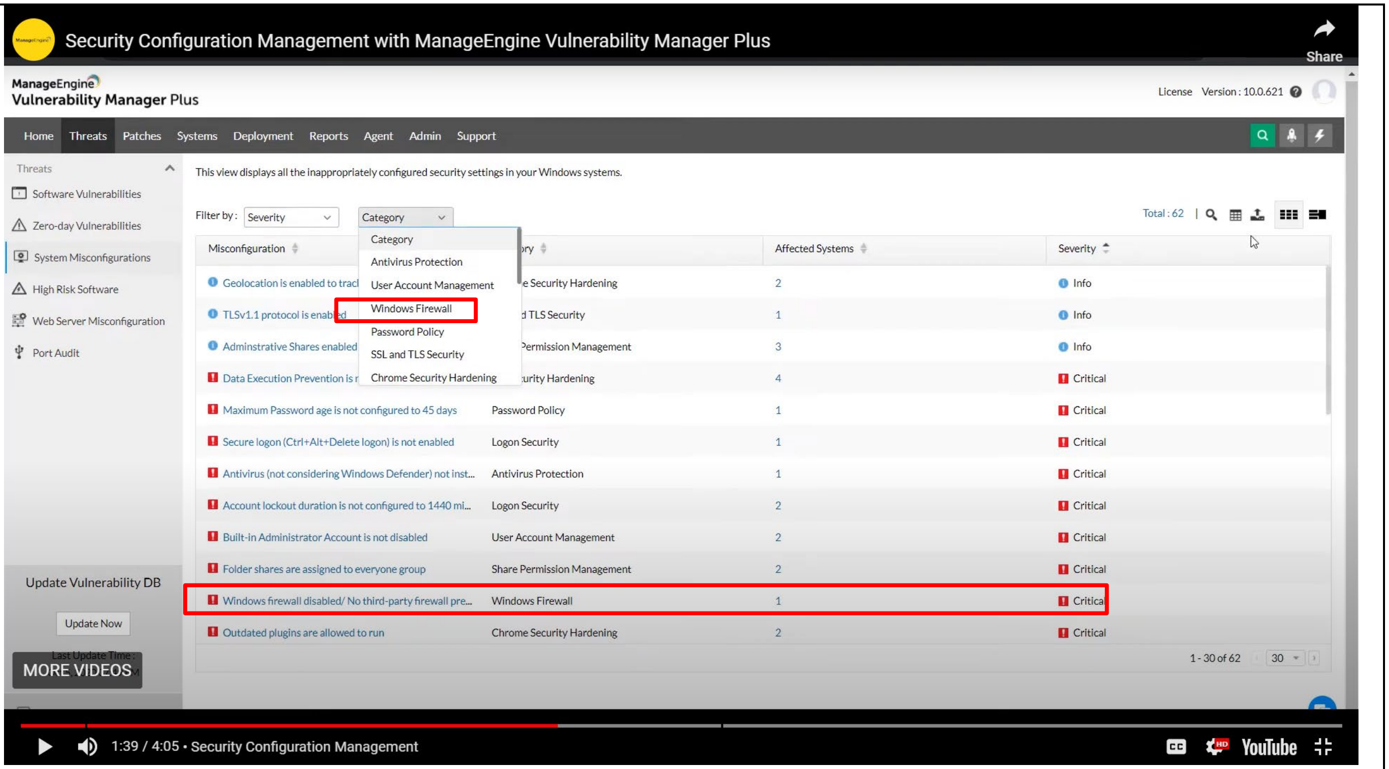
EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices	ManageEngine includes instructions to *cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type* (e.g., ManageEngine Vulnerability Manager Plus includes firewall option)*, a other occurrence mitigation type* (e.g., ManageEngine Vulnerability Manager Plus includes antivirus option). The ManageEngine provides flexibility to choose the devices for applying the different policies or mitigation techniques according to the requirements. Further, *across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices* (e.g., ManageEngine Vulnerability Manager Plus includes firewall option and the agent on each installed endpoint will actively scan the device details and remediated by deploying available remediation.). ManageEngine Vulnerability Manager Plus provide option to deploy patches and configuration from central dashboard. Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho



Security Configuration Management with ManageEngine Vulnerability Manager Plus

This view displays all the inappropriately configured security settings in your Windows systems.

Filter by : Severity | Category

Category
- Antivirus Protection
- User Account Management
- Windows Firewall
- Password Policy
- SSL and TLS Security
- Chrome Security Hardening

Total : 62

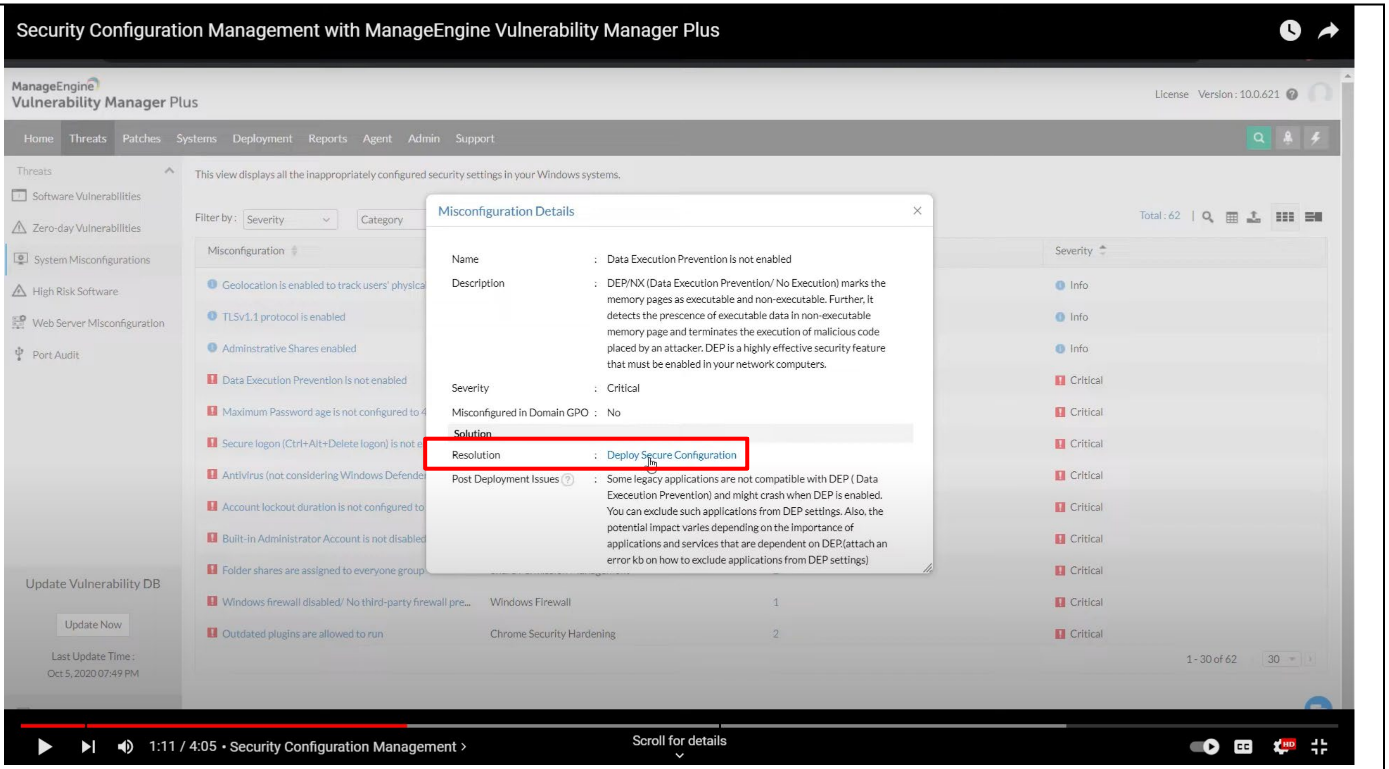
Misconfiguration	ory	Affected Systems	Severity
Geolocation is enabled to tracl	e Security Hardening	2	Info
TLSv1.1 protocol is enabled	d TLS Security	1	Info
Adminstrative Shares enabled	Permission Management	3	Info
Data Execution Prevention is r	urity Hardening	4	Critical
Maximum Password age is not configured to 45 days	Password Policy	1	Critical
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Logon Security	1	Critical
Antivirus (not considering Windows Defender) not inst...	Antivirus Protection	1	Critical
Account lockout duration is not configured to 1440 mi...	Logon Security	2	Critical
Built-in Administrator Account is not disabled	User Account Management	2	Critical
Folder shares are assigned to everyone group	Share Permission Management	2	Critical
Windows firewall disabled/ No third-party firewall pre...	Windows Firewall	1	Critical
Outdated plugins are allowed to run	Chrome Security Hardening	2	Critical

1 - 30 of 62 30

https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho



This view displays all the inappropriately configured security settings in your Windows systems.

Misconfiguration			Severity
Geolocation is enabled to track users' physica			Info
TLSv1.1 protocol is enabled			Info
Adminstrative Shares enabled			Info
Data Execution Prevention is not enabled			Critical
Maximum Password age is not configured to 4			Critical
Secure logon (Ctrl+Alt+Delete logon) is not e			Critical
Antivirus (not considering Windows Defende			Critical
Account lockout duration is not configured to			Critical
Built-in Administrator Account is not disabled			Critical
Folder shares are assigned to everyone group			Critical
Windows firewall disabled/ No third-party firewall pre...	Windows Firewall	1	Critical
Outdated plugins are allowed to run	Chrome Security Hardening	2	Critical

Misconfiguration Details

Name : Data Execution Prevention is not enabled

Description : DEP/NX (Data Execution Prevention/ No Execution) marks the memory pages as executable and non-executable. Further, it detects the prescence of executable data in non-executable memory page and terminates the execution of malicious code placed by an attacker. DEP is a highly effective security feature that must be enabled in your network computers.

Severity : Critical

Misconfigured in Domain GPO : No

Solution

Resolution : Deploy Secure Configuration

Post Deployment Issues : Some legacy applications are not compatible with DEP (Data Exeecution Prevention) and might crash when DEP is enabled. You can exclude such applications from DEP settings. Also, the potential impact varies depending on the importance of applications and services that are dependent on DEP.(attach an error kb on how to exclude applications from DEP settings)

https://www.youtube.com/watch?v=p2Oh87NruMo&t=53s

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

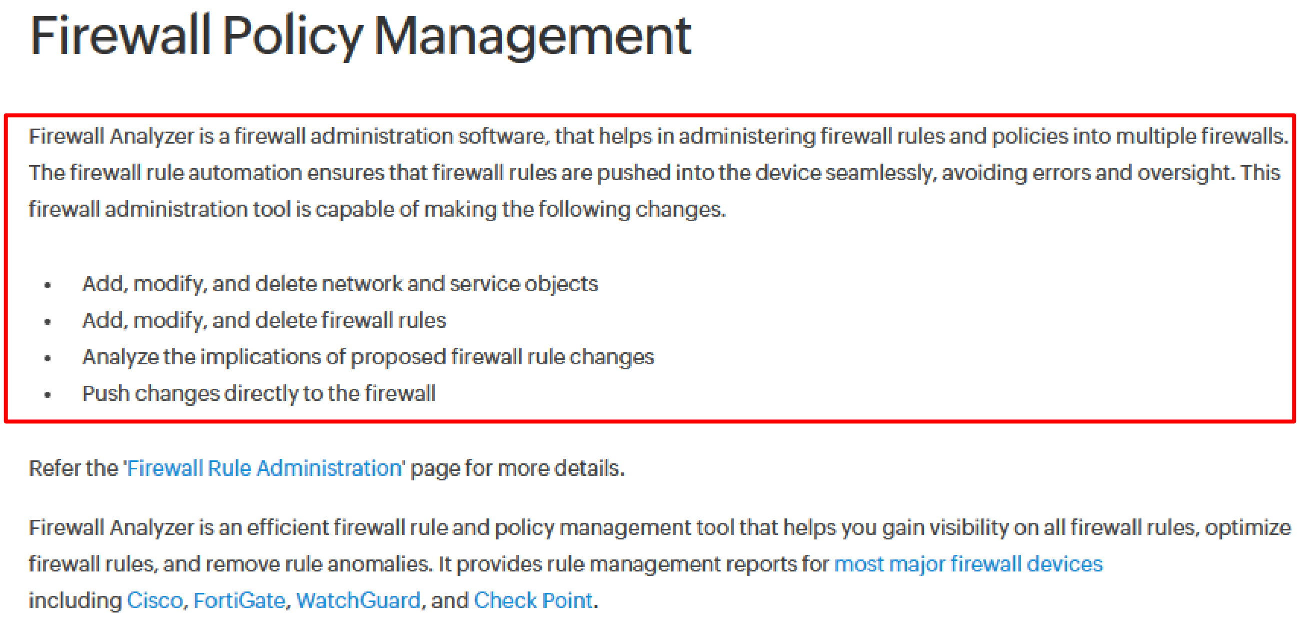
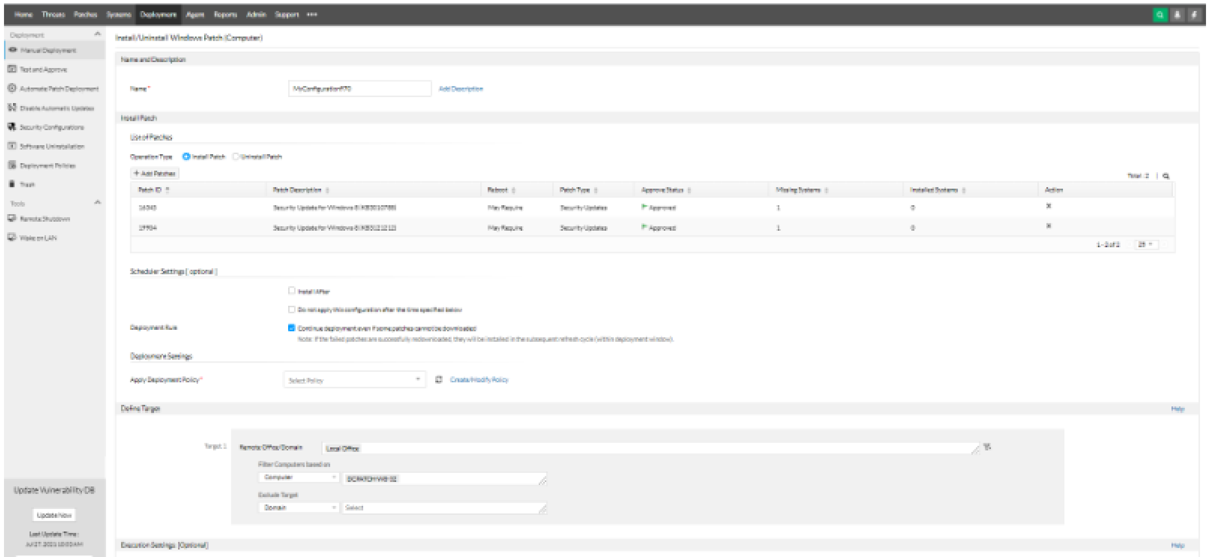
	 Firewall Policy Management Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes. - Add, modify, and delete network and service objects - Add, modify, and delete firewall rules - Analyze the implications of proposed firewall rule changes - Push changes directly to the firewall Refer the 'Firewall Rule Administration' page for more details. Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for most major firewall devices including Cisco, FortiGate, WatchGuard, and Check Point. https://www.manageengine.com/products/firewall/firewall-rule-management.html

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

Leverage built-in patching to ensure swift and accurate remediation

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.



Install/Uninstall Windows Patch (Computer)

Name and Description

Name* MyConfiguration##

Install Patch

List of Patches

Operation Type ● Install Patch ○ Uninstall Patch

Total : 2

Patch ID	Patch Description	Reboot	Patch Type	Approve Status	Missing Systems	Installed Systems	Action
16345	Security Update for Windows 8.1 KB3010788	May Require	Security Updates	Approved	1	0	☒
19904	Security Update for Windows 8.1 KB3121212	May Require	Security Updates	Approved	1	0	☒

1 - 2 of 2 25

Scheduler Settings [optional]

□ Install After

□ Do not apply this configuration after the time specified below

Deployment Rule ☑ Continue deployment even if some patches cannot be downloaded

Note: If the failed patches are successfully redownloaded, they will be installed in the subsequent refresh cycle (within deployment window).

Deployment Settings

Apply Deployment Policy* Select Policy

Define Target

Target 1 Remote Office/Domain Local Office

Filter Computers based on Computer SCRATCH-W8-32

Exclude Target Domain Select

Execution Settings [Optional]

Last Update Time : Jul 27, 2021 10:03 AM

https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

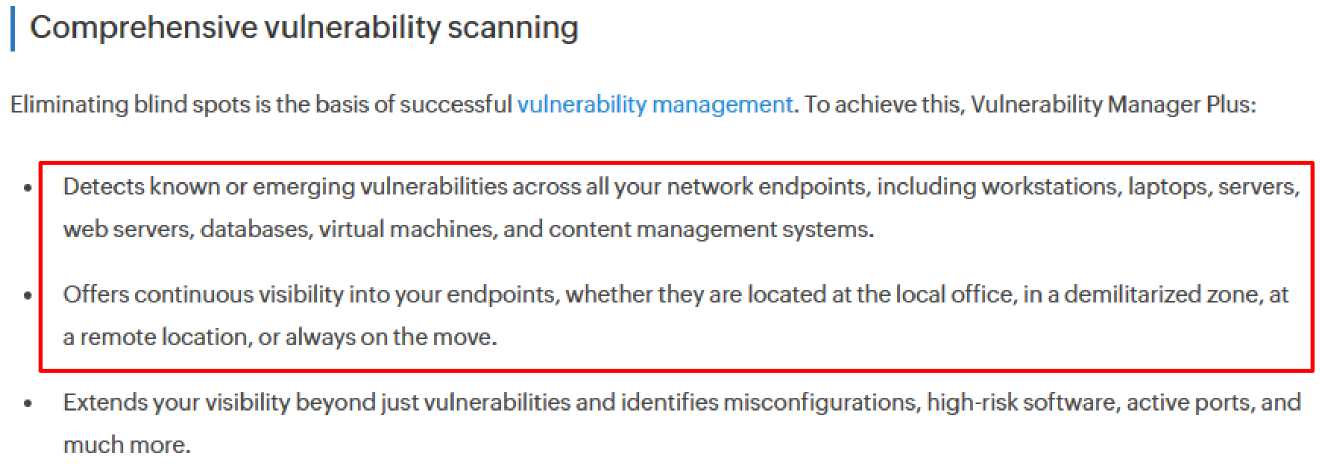
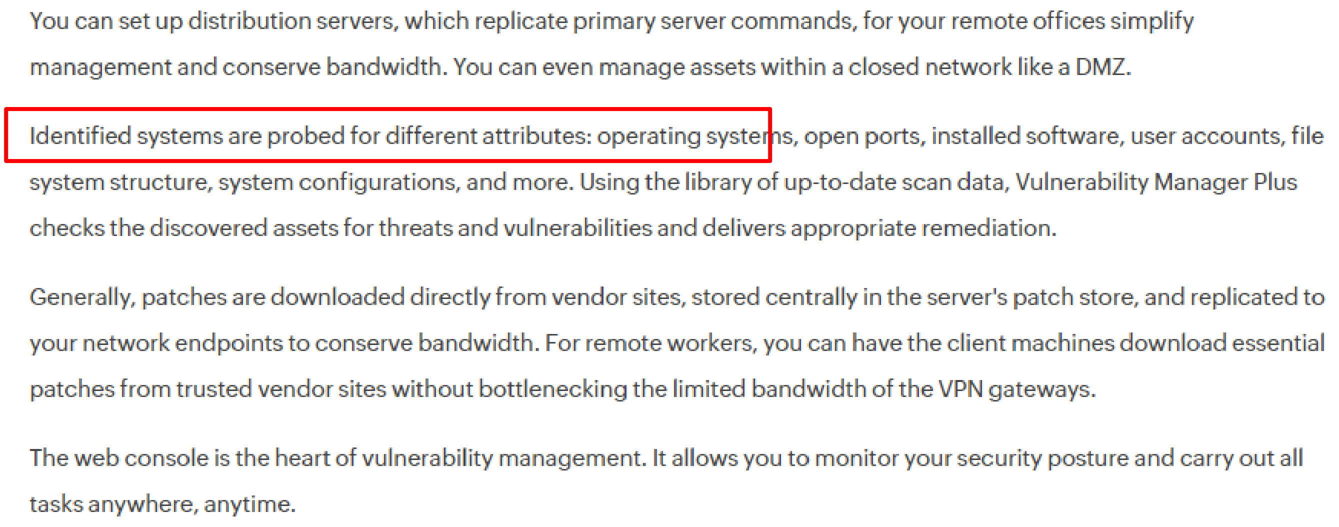
wherein the at least one configuration involves at least one operating system.	ManageEngine includes *least one configuration involves at least one operating system* (e.g., ManageEngine Vulnerability Manager Plus includes operating system information). Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):  Comprehensive vulnerability scanning Eliminating blind spots is the basis of successful vulnerability management. To achieve this, Vulnerability Manager Plus: • Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems. • Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move. • Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more. https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html

EXHIBIT 9

U.S. Patent No 10,893,066 v. Zoho

	 You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ. Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation. Generally, patches are downloaded directly from vendor sites, stored centrally in the server's patch store, and replicated to your network endpoints to conserve bandwidth. For remote workers, you can have the client machines download essential patches from trusted vendor sites without bottlenecking the limited bandwidth of the VPN gateways. The web console is the heart of vulnerability management. It allows you to monitor your security posture and carry out all tasks anywhere, anytime. https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html